PORTARIA CAAPSML-AT Nº 104, DE 11 DE MAIO DE 2026

SÚMULA: Institui e disciplina a Política de Segurança da Informação da Caixa de Assistência e Pensões dos Servidores Municipais de Londrina – CAAPSML.

O Superintendente da Caixa de Assistência, Aposentadorias e Pensões dos Servidores Municipais de Londrina - CAAPSML, no uso de suas atribuições legais, que lhe são conferidas pelo art. 158 da Lei Municipal nº 11.348, de 25 de outubro de 2011 e, considerando o previsto na Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709, de 14,08/2018,

RESOLVE:

Art. 1º - Aprovar a Política de Segurança da Informação, constituída por um conjunto de conceitos, objetivos, princípios, diretrizes, responsabilidades e vedações, de acordo com o Anexo I, desta Portaria.

Art. 2º – A presente Política de Segurança da Informação deve ser observada e respeitada como parte fundamental da cultura interna do da CAAPSML e, por tal razão, qualquer incidente que caracterize infringência às suas normas será ato contra as normas e políticas da Instituição.

Art. 3º – Esta Portaria entra em vigor na data da publicação, revogadas as disposições em contrário.

Luiz Nicácio

SUPERINTENDENTE

Documento assinado eletronicamente por **Luiz Nicacio**, **Superintendente**, em 11/05/2026, às 11:34, conforme horário oficial de Brasília, conforme a Medida Provisória nº 2.200-2 de 24/08/2001 e o Decreto Municipal nº 1.525 de 15/12/2017.

A autenticidade deste documento pode ser conferida no site http://sei.londrina.pr.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **18368743** e o código CRC **C3759FDA**.

ANEXO I

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - CAAPSML

DOS OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A política de segurança da informação visa garantir integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela instituição, devendo seguir os seguintes princípios básicos:

Confidencialidade: Proteção e garantia de que determinadas informações só são disponíveis a pessoas autorizadas.

Integridade: Garantia da exatidão das informações e dos métodos de processamento.

Disponibilidade: Garantia de que os usuários autorizados e os interessados tenham acesso às informações.

A Política de Segurança da Informação da CAAPSML almeja atender aos requisitos básicos definidos no manual do Pró-Gestão RPPS (versão 4.0-2025), sendo estes:

Nível I: Deve abranger todos os servidores e prestadores de serviço que acessem informações, indicando a responsabilidade de cada um quanto à segurança da informação.

Nível II: Adicionalmente aos requisitos do Nível I:

Indicar regras normativas quanto ao uso da Internet, do correio eletrônico e dos computadores e outros recursos tecnológicos.

Definir procedimentos de contingência, que determinem a existência de cópias de segurança dos sistemas informatizados e dos bancos de dados, o controle de acesso e a área responsável por elas, estando estes procedimentos mapeados e manualizados.

Nível III: Adicionalmente aos requisitos do Nível II, deverá contar com servidor ou área de Gestão da Segurança da Informação, com a responsabilidade de:

a) Prover todas as informações de Gestão de Segurança da Informação solicitadas pela Diretoria Executiva.
b) Prover ampla divulgação da Política e das Normas de Segurança da Informação para todos os servidores e prestadores de serviços.
c) Promover ações de conscientização sobre Segurança da Informação para os servidores e prestadores de serviços.
d) Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança dainformação.
e) Elaborar e manter política de classificação da informação, com temporalidade para guarda.

DAS DIRETRIZES E RESPONSABILIDADES

As políticas de segurança da informação de que trata este documento aplicam-se a todos os servidores, estagiários, prestadores de serviços e demais usuários que utilizem qualquer recurso informatizado físico ou lógico da CAAPSML, ou acesso às informações pertencentes à Autarquia.

As políticas de segurança da informação aqui tratadas observam o cumprimento das normas constantes no manual do Pró-gestão RPPS (versão 4.0 – 2025), bem como a Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) no Município, e Decreto 214/2021. O descumprimento dessas normas, ficará submetido à legislação em vigor.

Aplica-se ainda ao gerenciamento de quaisquer equipamentos, programas, meios físicos de tráfegos e sistemas de armazenamento digital de dados e informações incluindo notebooks, tablets, unidades móveis de armazenamento (discos rígidos- HDs), smartphones, impressoras, além das estações de trabalho, inseridos nas dependências da CAAPSML.

É de responsabilidade dos responsáveis pela área de Segurança da Informação publicar e promover as versões da Política de Segurança de Informação, bem como conscientizar os colaboradores em relação à relevância da Segurança da Informação para a o bom funcionamento da Autarquia, atendendo as legislações e regulamentos da Prefeitura Municipal de Londrina, bem como a Lei Geral de Proteção de Dados vigente.

A configuração de todos os equipamentos, ferramentas e sistemas para que fiquem de acordo com as normas estabelecidas pela Política de Segurança da Informação, é de responsabilidade da Caixa de Assistência e Pensões dos Servidores Municipais de Londrina - CAAPSML, por meio do suporte técnico da Diretoria de Tecnologia e Informação/SMPOT, de acordo com as práticas preconizadas por normas e modelos de referência relativos ao tema.

Cada servidor deverá possuir sua própria senha com os devidos privilégios, composta, preferencialmente, por oito dígitos com ao menos um caractere maiúsculo e um especial. Devendo ser destacado que caso a senha seja compartilhada, a responsabilidade por eventuais alterações, inclusões ou qualquer outra atividade efetivada com a mesma será do detentor original da senha.

A senha do administrador do sistema só deverá ser solicitada quando estritamente necessária, como

no caso, por exemplo, de downloads, manutenção, atualização ou instalação de programas essenciais à elaboração de tarefas. Os privilégios de administrador só serão aceitos e cedidos após análise e validação da causa, de acordo com as regras do Município de Londrina, para seus servidores.
O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções.
Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados. A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função.
A padronização deverá ser utilizada com o fim de garantir integridade, melhor acessibilidade e facilidade em todos os processos envolvendo Tecnologia da Informação.
É obrigatória a “salva” regular programada de arquivos, independente do tamanho, devendo ser observada junto com a DTI/SMPOT as possibilidades para realização de backup.
As regras atuais da Política de Segurança de Informação estabelecidas pela CAAPSML tem o objetivo de estimular o desenvolvimento de um comportamento ético e profissional do uso da internet.

DO USO DA INTERNET

O acesso à internet está disponível aos servidores e estagiários a partir das estações de trabalho da Autarquia.
A internet disponibilizada pode ser usada com finalidade pessoal, desde que não prejudique a produtividade da unidade e não onere a rede, causando lentidão ou outros problemas. Da mesma forma, seu uso não deve ferir qualquer norma do Código de Ética vigente.
É proibida a divulgação de qualquer informação corporativa em redes sociais, listas de discussão, comunidades de relacionamento ou a terceiros via comunicadores eletrônicos ou qualquer outra tecnologia que venha surgir da internet, salvo quando realizado pelas pessoas autorizadas a realizar comunicação externa.
É proibido o *download* e a instalação de softwares que tenham direitos autorais, marca registrada ou patente na internet e que não foram devidamente adquiridos pela autarquia. O mesmo se aplica ao download de mídias e arquivos em geral que não sejam de uso livre, sejam eles imagens, apresentações, planilhas, músicas, entre outros.
É proibido expor, armazenar, distribuir, editar, imprimir ou gravar materiais de cunho sexual, obsceno, difamatório, ofensivo, preconceituoso e político (propaganda) por qualquer meio.
É permitido aos colaboradores usar a conexão wifi, desde que complacentemente com as normas do Código de Ética.

DA REDE - XINGU

O uso da rede “Xingu” é permitido a todos os usuários. Entretanto, os diretórios existentes ali estão permissionados de acordo com o organograma vigente na Autarquia.
Caso haja alguma necessidade de alteração no permissionamento, esta deverá ser comunicada e justificada à Diretoria de Tecnologia da Informação – SMPOT via processo específico do SEI.
Além dos diretórios correspondentes às unidades, existem os diretórios de compartilhamentos, nos quais os usuários podem compartilhar arquivos com outros.
Não é permitido armazenar arquivos que não tenham relação com o trabalho realizado, especialmente filmes e músicas, ainda que aparentemente não cause prejuízo à instituição.
É vedado:

· Armazenar vídeos e músicas;

· Armazenar conteúdo difamatório, ofensivo, preconceituoso, obsceno, sexual, calunioso ou que tenha fins de propaganda política;

· Editar ou apagar arquivos de outros usuários sem autorização do mesmo;

· Fraudar, de qualquer forma, as informações dos arquivos;

· Instalar ou armazenar programas sem o conhecimento da DTI;

· Armazenar conteúdo nocivo, como vírus e *malwares*;

· Armazenar conteúdo protegido por direitos autorais ou patentes.

Qualquer necessidade de armazenamento de arquivo que se configure como exceção às regras apresentadas deve ser comunicada à área de TI para avaliação, desde que haja justificativa plausível.

DO CORREIO ELETRÔNICO

O uso do correio eletrônico da CAAPSML é para fins corporativos e relacionados às atividades do colaborador usuário. A utilização desse serviço para fins pessoais é permitida desde que seja feita com bom senso e sem conflito com qualquer norma do Código de Ética, não prejudique a autarquia e nem cause impacto no tráfego da rede.

É vedado aos colaboradores da CAAPSML:

· Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Autarquia;

· Enviar mensagens usando nome de usuário de outra pessoa ou endereço eletrônico que não esteja autorizado a usar;

· Enviar qualquer e-mail que torne seu remetente e/ou a CAAPSML vulneráveis a ações civis ou criminais;

· Divulgar externamente informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização explícita;

· Produzir, transmitir ou divulgar mensagem que:
  - ü Conflite com os interesses da autarquia;
  - ü Contenha ameaças eletrônicas, como spam ou vírus;
  - ü Vise obter acesso não autorizado a outro computador ou servidor;
  - ü Vise interromper um serviço por meio de método ilícito;
  - ü Vise burlar qualquer sistema de segurança;
  - ü Vise vigiar secretamente ou assediar outro usuário;
  - ü Vise acessar informações confidenciais sem autorização explícita do proprietário;
  - ü Possua anexo superior a 10MB;
  - ü Tenha conteúdo considerado impróprio, obsceno ou ilegal;
  - ü Seja caluniosa, difamatória ou ofensiva;
  - ü Tenha fins políticos (propaganda);
  - ü Inclua material protegido por direitos autorais sem a permissão do detentor.

Toda mensagem enviada pelo correio eletrônico deve possuir uma assinatura que identifique

claramente o remetente.

DO BACKUP (CÓPIA DE SEGURANÇA)

A segurança e integridade dos dados são prioridades fundamentais na infraestrutura de tecnologia. Para assegurar essa proteção, rotinas de backup automáticas foram implementadas.
No que diz respeito aos arquivos armazenados no servidor central, sob responsabilidade da DTI, foi adotada uma abordagem proativa, com rotinas automáticas de backup que garantem que todos os diretórios.
Essa prática elimina a necessidade de intervenção humana, proporcionando uma camada adicional de segurança contra possíveis falhas de hardware.
No âmbito do sistema previdenciário e de folha de pagamento, a empresa Actuary Assessoria Atuarial e Informática realiza a gestão dos dados sensíveis. Há um protocolo de backup automático que, de forma programada e sem intervenção manual, realiza cópias regulares da base de dados. Essa prática é essencial para assegurar a integridade das informações relacionadas às obrigações previdenciárias e folha de pagamento.

DO CONTROLE DE ACESSO FÍSICO
O acesso às áreas críticas, como salas de servidores e racks de rede, é restrito a servidores autorizados.
Documentos físicos contendo dados pessoais ou sensíveis devem ser armazenados em mobiliário com controle de acesso, que será realizado pela Gerência Administrativa Previdenciária.
É vedada a retirada de documentos das dependências da Autarquia sem autorização formal da Gerência Administrativa Previdenciária.

DA CLASSIFICAÇÃO, TEMPORALIDADE E GUARDA DA INFORMAÇÃO
As informações da CAAPSML devem ser classificadas conforme grau de sensibilidade, observando critérios de acesso, guarda e descarte.
Considerando a natureza previdenciária da Autarquia:

- documentos relativos a segurados, benefícios, folha de pagamento, arrecadação e atos normativos são de guarda permanente;
- documentos digitais devem ser preservados com adoção de medidas para evitar obsolescência tecnológica.

DA GESTÃO DE RISCOS E INCIDENTES DE SEGURANÇA FÍSICA

Do Controle de Acesso Físico
O acesso às áreas consideradas críticas para a segurança da informação — incluindo, mas não se limitando a salas de servidores, data centers, racks de rede, salas técnicas, arquivos permanentes e quaisquer ambientes que abriguem infraestrutura tecnológica ou ativos de informação sensíveis — é terminantemente restrito a servidores formalmente autorizados, mediante designação expressa da autoridade competente e registro prévio de acesso.
O controle de acesso físico deverá observar critérios de necessidade funcional, segregação de funções e rastreabilidade, sendo vedado o acesso genérico ou irrestrito.
O ingresso de terceiros, visitantes, fornecedores ou prestadores de serviços em áreas críticas somente será permitido em caráter excepcional, mediante autorização formal, específica e previamente registrada, devendo ocorrer sob acompanhamento contínuo de servidor designado, que responderá solidariamente por eventuais irregularidades.

Da Proteção de Documentos Físicos e Ativos de Informação
Os documentos físicos que contenham dados pessoais, dados sensíveis, informações previdenciárias, financeiras, administrativas ou quaisquer informações classificadas deverão ser obrigatoriamente

armazenados em mobiliário apropriado, dotado de mecanismos de trancamento e controle de acesso, sob responsabilidade direta da Gerência Administrativa Previdenciária.
Compete à Gerência Administrativa Previdenciária:
I – definir os níveis de acesso aos documentos físicos;
II – manter relação atualizada dos servidores autorizados;
III – fiscalizar o cumprimento das normas de guarda, manuseio e preservação;
IV – adotar medidas corretivas em caso de não conformidade.
É expressamente proibida a retirada, empréstimo, transporte, reprodução ou cópia de documentos físicos pertencentes à CAAPSML para fora de suas dependências sem autorização formal, específica e previamente concedida pela Gerência Administrativa Previdenciária, devendo a autorização conter, no mínimo:

- a identificação do responsável;
- a finalidade da retirada;
- o prazo de permanência fora da Autarquia;
- as condições de guarda, transporte e devolução.

Do Gerenciamento de Riscos de Segurança Física
A CAAPSML deverá identificar, avaliar e tratar, de forma sistemática e contínua, os riscos relacionados à segurança física dos ativos de informação, considerando ameaças como acesso não autorizado, extravio, dano físico, sabotagem, sinistros e desastres.
As medidas de mitigação de riscos incluem, entre outras:

- controle e registro de acessos físicos;
- restrição de circulação em áreas sensíveis;
- segregação de ambientes;
- definição de responsáveis pelos ativos;
- integração das ações de segurança física com os planos de contingência e continuidade.

Da Gestão de Incidentes de Segurança Física
Todo evento ou suspeita de violação das regras de acesso físico, extravio de documentos, acesso não autorizado a áreas restritas, dano ou comprometimento de ativos físicos de informação deverá ser **imediatamente comunicado** à área de Gestão da Segurança da Informação e à Gerência Administrativa Previdenciária para registro, análise e adoção das medidas cabíveis.
Os incidentes de segurança física deverão:
I – ser formalmente registrados;
II – ter suas causas analisadas;
III – gerar ações corretivas e preventivas;
IV – ser reportados à Diretoria Executiva quando apresentarem risco relevante, impacto institucional ou envolvimento de dados pessoais, nos termos da LGPD.

Das Responsabilidades e Sanções
O descumprimento das normas relativas à gestão de riscos e incidentes de segurança física constitui infração administrativa e sujeita o responsável às sanções previstas na legislação vigente, sem prejuízo da apuração de responsabilidades civis e penais.
Todos os servidores, estagiários, prestadores de serviços e terceiros são corresponsáveis pela preservação da segurança física dos ativos de informação e pelo cumprimento das diretrizes estabelecidas nesta Política.

BOAS PRÁTICAS

No dia-a-dia, os colaboradores da CAAPSML devem observar e praticar os seguintes hábitos:

- Retirada dos papéis da impressora: toda vez que alguém enviar um documento para impressão, o mesmo deve ser retirado imediatamente, de forma a evitar que ele fique exposto a terceiros;

- Descarte de papéis: caso algum papel com informação relevante e/ou confidencial necessite ser descartado, ele deve ser rasgado antes do descarte. Documentos confidenciais ou com dados pessoais de segurados não devem ser utilizados como papel de rascunho, devendo ser realizado o descarte apropriado;

- Bloqueio da estação de trabalho: ao ausentar-se da sua estação de trabalho sem bloquear a tela do computador, o usuário está aceitando o risco de um terceiro utilizar sua máquina sem autorização. Assim, o bloqueio deve ser feito após qualquer saída de frente da estação de trabalho. A proteção de tela também deve ser configurada para que o micro seja bloqueado após determinado período de inatividade;

- Retirada de documentos da sede: não se deve retirar documentos da sede da CAAPSML, pois uma vez fora do prédio não é possível garantir seu correto tratamento. Caso haja a necessidade de locomoção dos documentos para reuniões externas ou viagens, a gerência responsável pela respectiva guarda deve ser informada.

CONSIDERAÇÕES FINAIS

Os casos omissos serão avaliados pela Superintendência, pela área de Gestão da Segurança da Informação e pelas unidades competentes, observadas a legislação vigente, as normas municipais, os princípios da administração pública e as diretrizes do Pró-Gestão RPPS.

Esta Política entra em vigor na data de sua aprovação, devendo ser divulgada aos usuários abrangidos e publicada em meio oficial, sem prejuízo da elaboração de normas complementares, manuais operacionais, fluxos, formulários, matrizes de acesso e planos de ação necessários à sua execução.

Esta Política deverá ser revisada periodicamente, preferencialmente a cada dois anos, ou antes desse prazo quando houver alteração normativa relevante, mudança tecnológica, reestruturação organizacional, recomendação de auditoria, ocorrência de incidente significativo ou necessidade de adequação ao Pró-Gestão RPPS.